UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

YOLANDA XIONG on behalf of herself and all others similarly situated, Plaintiff, v. NETGAIN TECHNOLOGY, LLC, Defendant.	Case No. 22-cv-01826 CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

Plaintiff Yoland Xiong individually and on behalf of all others similarly situated, by and through her attorneys, brings this class action against Netgain Technology, LLC ("Netgain" or "Defendant"), upon personal knowledge as to herself and her own acts and experiences, and upon information and belief as to all other matters, including her counsel's investigation, allege as follows. Plaintiff believes additional evidentiary support exists for her allegations, given an opportunity for discovery.

INTRODUCTION AND NATURE OF ACTION

1. Netgain is an external IT vendor providing "secure and scalable" information technology ("IT") and cloud-computing services for businesses. Netgain provides cloud-enabled IT solutions and managed services to various types of business entities. Specifically, Netgain specializes in serving the IT needs of two highly specialized and regulated industries: health care and accounting. Under Netgain's IT services model, its clients move their IT infrastructure into a cloud-based system managed, overseen and used by Netgain to serve its clients' specific IT needs.

2. Because it specializes in healthcare and accounting, Netgain is responsible for managing and overseeing highly sensitive data. Its clients collect, store, and use personal and confidential information that includes names, addresses, social security numbers, medical records and histories, and financial account information. As Netgain itself acknowledged, this type of personal and sensitive data is highly targeted by hackers seeking to exploit that data for nefarious purposes. For example, fraudsters utilize medical information to secure medical procedures and bill the victim, attempt to utilize financial information to make fraudulent transactions and purchases, or use a collection of personal data to take out fraudulent loans. In the wrong hands, these types of sensitive, personal data may be wielded to cause significant harm to the patient or individual whose information is described in the records that Netgain, through its clients, stores.

3. Netgain assures its clients that it is a sophisticated cybersecurity company capable of keeping its clients' records (and the patients and individuals whose information is described in those records) safe. In fact, Netgain represented its services as "DoD-grade" providing "ultra-secure protection" to its clients' data. Netgain also frequently published cybersecurity-related webinars stressing the importance of maintaining adequate data security and offering advice on how to keep data safe and prevent a data breach.

4. Indeed, Netgain has provided IT solutions and cybersecurity services for organizations for almost 20 years, and has offices and data centers in Chicago, Minneapolis, San Diego, and Phoenix. It is, moreover, a sophisticated company with

approximately 130 employees across its locations, and its IT and cyber services generate $32.35 million dollars in sales.[1]

5. In reality, Netgain's self-depiction as a cybersecurity expert proved false. Contrary to its many representations and promises, Netgain utilized inadequate data security measures it knew, or should have known, put the highly sensitive data entrusted to it at significant risk of theft by or exposure to nefarious parties. Netgain, moreover, failed to meet the very cybersecurity standards that it underscored as critical for its clients' businesses.

6. In late September 2020, due to Netgain's inadequate data security and failure to comply with federal and state data privacy standards, an unauthorized third party used compromised credentials to gain access to Netgain's digital environment. Thereafter, the unauthorized third party gained access to and exfiltrated the files and records of at least 15 of Netgain's customers. However, Netgain, more than a year and a half after the Data Breach, is continuing to disclose which of its customers were impacted.

7. With the sensitive files and records secured and stolen, the hackers purportedly issued a ransom demand to Netgain. Netgain claimed to have paid an undisclosed amount to the cybercriminal in exchange for assurances that the criminal would delete all copies of the data obtained and that it would not publish, sell, or otherwise

[1] *Netgain Technology, LLC*, D&B Bus. Directory (last visited, Sept. 22, 2021), https://www.dnb.com/business-directory/company-profiles.netgain_technology_llc.52f33163cb3c315c73f15169f269e977.html

disclose the data. However, Netgain has provided no public information on the ransom demand. This series of events is referred to herein as the "Data Breach."

8. Plaintiff brings this class action against Netgain for its failure to secure and safeguard the confidential, personally identifiable information of hundreds of thousands of consumers. The categories of stolen information included names, account numbers, Social Security numbers, driver's license numbers, bank account numbers, and dates of birth ("Personally Identifying Information" or "PII"). Because Netgain also had healthcare-industry clients, the exfiltrated data included some individuals' health information such as medical record numbers, health insurance policy and identification numbers, clinical notes, referral requests, laboratory reports, decision not to vaccinate forms, immunization information, medical disclosure logs, in addition to other medical or health related information ("Private Health Information" or "PHI"). PII and PHI is collectively referred to as Sensitive Information.

9. Due to Netgain's negligence, Plaintiff and the Class have suffered harm and are subject to a present and continuing risk of identity theft. Plaintiff and the Class's Sensitive Information has been compromised and they must now undertake additional security measures to mitigate the damage caused by Defendant's actions.

10. The Data Breach impacted many of Netgain's clients, especially those in the healthcare industry, and those clients have already indicated that hundreds of thousands of records were stolen. The full scope of the Data Breach, however, is either not known or has not been publicly disclosed. In fact, Netgain appears to still be identifying which of its clients were affected by the Data Breach. On May 28, 2021, months after the Data Breach,

Netgain issued a notice to one of its former clients, Caravus, warning that Caravus's clients' data was exposed during the breach. Additionally, on August 24, 2021, one of Netgain's clients, LifeLong Medical Care, first reported that Netgain provided notice that its clients' Sensitive Information was impacted by the Data Breach. More recently, in January 2022, Entira Family Clinics issued notices to victims notifying them for the first time that their information was impacted by Netgain's Data Breach, which occurred more than a year before.

11. Plaintiff brings this Complaint on behalf of persons whose Sensitive Information was stolen during the Data Breach. Plaintiff asserts claims for negligence and declaratory and injunctive relief.

JURISDICTION AND VENUE

12. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one member of the class and Defendant are citizens of different states. There are more than 100 putative members of the Class.

13. This Court has jurisdiction over Defendant because it maintains its principal place of business in Minnesota, regularly conducts business in Minnesota, and has sufficient minimum contacts in Minnesota. Defendant intentionally availed itself of this jurisdiction by marketing and selling products and services from Minnesota to many businesses nationwide.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

15. Plaintiff Yolanda Xiong is a resident of Maplewood, Minnesota. She received notice from a healthcare provider, Entira Family Clinics ("Entira"), that her information was at risk due to the Netgain Data Breach. Plaintiff Xiong has been a patient at Entira for approximately 12 years. Plaintiff Xiong suffered identity theft following the Data Breach, receiving a letter from a credit bureau informing her that attempts were made to open credit card accounts in her name.

16. Defendant Netgain Technology, LLC is an American cloud-based IT services provider based in St. Cloud, Minnesota and incorporated in Delaware.

FACTUAL BACKGROUND

17. Netgain is a company located in St. Cloud, Minnesota, which externally manages IT and cloud computing services on behalf of companies primarily in the healthcare and accounting industries. This includes managing and overseeing highly sensitive data.

18. Netgain was founded in 2000 under the premise "that there had to be a better way to implement, manage and support IT."[2] Netgain proclaims to have revolutionized the industry for support and help desk experiences for organizations across various industries.

[2] *History*, NetgainCloud.com (last visited, Sept. 22, 2021), https://netgaincloud.com/about-us/history/.

Specifically, Netgain specialized in providing IT services to healthcare and financial service companies, two areas that require storing and managing highly sensitive personal information. As a provider of cybersecurity solutions, among other IT services, in the heavily regulated healthcare and financial fields maintaining PII, PHI, and other Sensitive Information, Netgain had a duty to safeguard the data provided by the organizations who were receiving or had received its services. Plaintiff and the Class had a reasonable expectation that the highly Sensitive Information provided to healthcare and financial companies impacted by the Data Breach would be protected. Netgain, as the holder of that Sensitive Information, had an obligation to reasonably protect it against theft and misuse.

19. As detailed more fully below, Netgain failed to safely and securely store the Sensitive Information entrusted to it and failed to prevent it from being compromised during the Data Breach.

A. The Data Breach

20. Netgain claims to be the industry standard for secure and scalable IT-as-a-Service ("ITaaS") for accounting and healthcare businesses.[3] Netgain's ITaaS business model includes moving its clients' IT infrastructure "into a secure, cloud-based opex solution" allowing Netgain to tailor IT services specific to each clients' needs.[4] In other words, Netgain replaces traditional internal IT departments and, in addition to managing traditional IT needs, provides a host of other IT-related services, including, for example,

[3] *Id.*; *see also It-As-A-Service,* NetgainCloud.com (last visited Sept. 22, 2021), https://netgaincloud.com/it-as-a-service/

[4] *IT-As-A-Service*, NetgainCloud.com (last visited, Sept. 22, 221), https://netgaincloud.com/it-as-a-service/

cloud computing, technical infrastructure, IT management, and service and application management and security. As such, Netgain is well aware the accounting and healthcare industries it services process some of the most valuable and targeted data for cybercriminals.

21. Netgain claims its ITaaS services offer a "better way" to deliver IT that allows it to "closely partner with accounting and healthcare clients to help navigate the industry's complex technological challenges and increasing regulations."[5] Netgain purports to offer "deep experience and specialization" and represents that its "IT and support professionals are fully committed to ensuring that [its clients] are pleased and [their] needs are fully met."[6]

22. Netgain also "pledge[s] to [its] clients that when they partner with Netgain, [its] team will deliver" and promises to, among other things: "Bring a business perspective and share exactly how the solutions will protect and support your business objectives and goals," "Remain on the leading edge of technology and stay current with the ever-changing needs and requirements of accounting and healthcare," and "Confirm your IT is running smoothly, and help to eliminate issues and loss of productivity."[7] Netgain states that its "Vision" is to serve "customers in industries characterized by high compliance and high

[5] *About Us*, NetgainCloud.com (last visited, Sept. 22, 2021), https://netgaincloud.com/about-us/
[6] *Id.*
[7] *Id.*

security" and that it provides its clients with "better technical knowledge, expertise, execution and confidence[.]"[8]

23. Netgain's ITaaS services are specialized for businesses who manage highly sensitive data, specifically, businesses in the healthcare and accounting industries. Netgain, in fact, describes itself as a "leading outsourced provider of IT-as-a-Service" to customers in healthcare and accounting. Netgain, thus, must oversee, manage, and protect its clients' sensitive data that includes personally identifying information (like names, addresses, and social security numbers), healthcare information (like medical records and histories), and financial information (like payroll data and banking account information).

24. Given the highly sensitive nature of its clients' businesses, Netgain understood the need to protect its clients' data and prioritize its data security. In fact, in 2017—long before Netgain's Data Breach—Netgain warned of the substantial costs of a data breach generally, and of a breach in the healthcare industry specifically.[9] It noted that a data breach could cost healthcare companies approximately $380 per record exposed, and $141 per record in other industries.[10]

25. Netgain explained that, in particular, "[m]edical records are incredibly valuable to hackers because the data (names, addresses, social security numbers, medical

[8] *Id.*
[9] *Understanding the True Cost of a Data Breach*, Netgain (Nov. 17, 2017), https://netgaincloud.com/blog/infographic-understanding-true-cost-data-breach-healthcare/
[10] *Id.*

history, insurance information, etc) is not easily changed."[11] As such, Netgain noted the healthcare industry annually spent over $6.2 billion on data breach-related costs.[12]

26. In the face of the risks of a data breach, Netgain advised that "Protecting your practice is crucial" and that "appropriate administrative and technical controls will mitigate your practice's vulnerability[.]"[13] Netgain provided examples of the types of controls that businesses should adopt, including: (1) "Administrative Controls" like "conducting regular user training, hiring a dedicated security officer; (2) employing and enforcing Bring Your Own Device (BYOD) policies; (3) conducting extensive due diligence on third-party vendors"; and (4) "Technical Controls" like "patching and updating systems, automating your disaster recovery process and using anti-malware software."[14] Netgain also warned that compliance failures and failing to extensively use encryption would increase the costs of a data breach.[15]

27. Netgain portrayed itself as a data security expert to its clients and the public. It provided a host of cybersecurity-related webinars and presentations to its clients, including "Security Awareness Training," "Staying out of the Cybersecurity Headlines: Protecting Your Internal Cybersecurity Protects Your Organization," "Cybersecurity and

[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.*

Risk Management in 2020 – Planning and Protecting Your Firm," and "The Costs of Bad Security and How it Affects Your Organization."[16]

28. Netgain further represented that it was fully capable of securing clients' highly sensitive medical and accounting data. As shown in **Image 1** below, Netgain advertised that "The Netgain Standard is included with every solution. Every time." The "Netgain Standard" including, among other things, "Cybersecurity," where Netgain promised to "Safeguard [clients'] sensitive data from tomorrow's threats with DoD-grade, ultra-secure protection."[17]

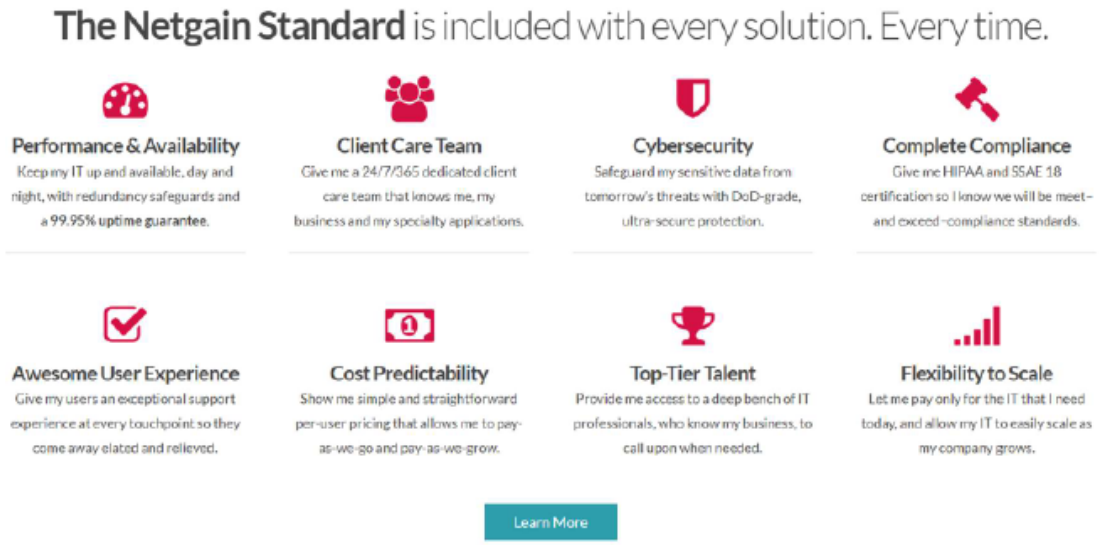

Image 1. Description of "The Netgain Standard."

[16] *Cybersecurity Webinars*, NetgainCloud.com (last visited, Sept. 22, 2021), https://netgaincloud.com/webinar/cybersecurity-webinars/
[17] *The Netgain Standard*, NetgainCloud.com (last visited, Sept. 22, 2021), https://netgaincloud.com/why-netgain/

29. Netgain also claimed it is "always there to keep your IT secure, available and performant."[18] As shown in **Image 2** below, Netgain's cybersecurity page states that: "Hackers don't sleep. But you can" and, further, that "Our security approach enables you to meet-and often exceed- compliance requirements while providing your staff with secure access to the information they need to do their jobs."[19]

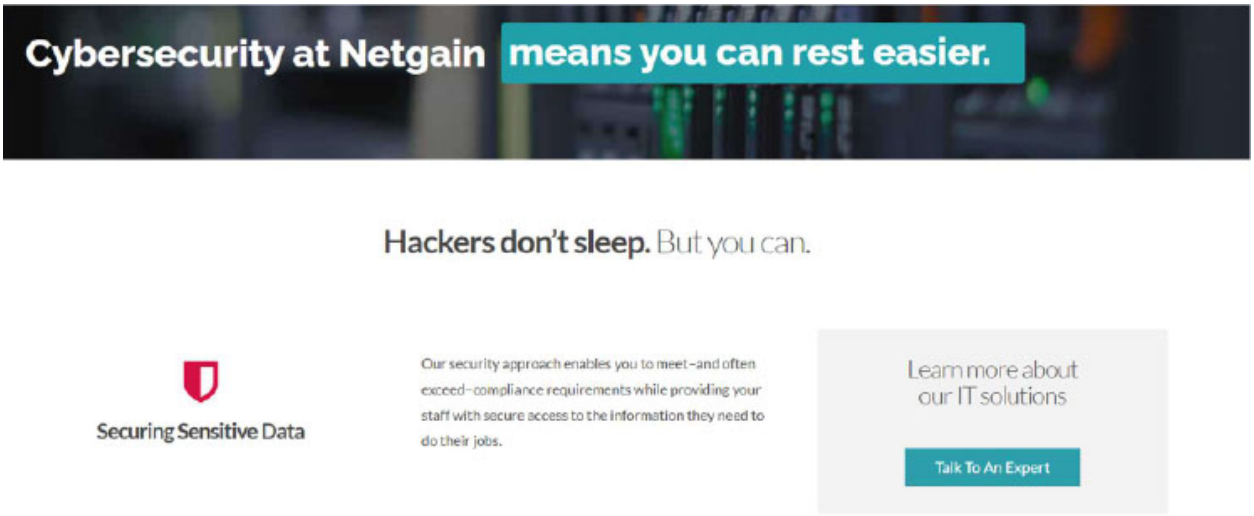

Image 2. A picture of Netgain's advertisement related to its cybersecurity services.

30. In fact, Netgain touts its data security measures are like "Housing user data within the granite confines of a former Federal Building" that "ensures a level of structural stability that our clients trust."[20] Yet, while its customers reasonably believed their data

[18] *About Us*, NetgainCloud.com (last visited, Sept. 22, 2021), https://netgaincloud.com/about-us/
[19] *Cybersecurity at Netgain*, NetgainCloud.com (last visited, Sept. 22, 2021), https://netgaincloud.com/cybersecurity/
[20] *About Us*, NetgainCloud.com (last visited, Sept. 22, 2021), https://netgaincloud.com/about-us/

was safe within Netgain's confines, between September 2020 and November 2020 Netgain's guard was down and cyber criminals infiltrated its walls.

31. Although Netgain's business involves providing IT services related to the storage and maintenance of highly sensitive data, it implemented inadequate data security practices that, as a purported cybersecurity expert, it knew or should have known, put its clients and their customers at risk of having their sensitive data exposed.

32. In the leadup to the Data Breach, Netgain was disorganized, had an incredibly high rate of employee turnover, and had extensive problems meeting deadlines and addressing client concerns.[21] These organizational difficulties were a red flag that either did or should have put Netgain on notice that its systems were vulnerable to attack and that it had not adequately staffed or supported a secure environment.

33. From September to December 2020, Netgain was subjected to a ransomware attack that targeted Netgain's domain controllers, which managed networks of thousands of servers. Included in the ransomware attack was the Sensitive Information provided to Netgain by certain of its clients. Shortly thereafter, Netgain began emailing its clients that it was going to shut down data centers in an effort to isolate the ransomware and rebuild the affected systems.

34. As a third-party IT service provider, Netgain had access to and controlled data from many, if not all, of its clients. That data was stored on Netgain's servers. Netgain, thus, held a "master key" capable of "unlocking" each of its clients' "locks" put in place to

[21] Netgain Reviews, glassdoor, https://www.glassdoor.com/Reviews/Netgain-Reviews-E454747.htm (last visited September 22, 2021).

protect the highly sensitive data stored on its servers. By breaching Netgain, the hackers gained access to Netgain's past and present clients' data that Netgain oversaw and managed.

35. According to one of Netgain's clients, the hackers accessed portions of Netgain's data environment and successfully exfiltrated data out of Netgain's system.[22] In other words, the attack successfully resulted in the theft of critical, sensitive data. The types of data confirmed or otherwise suspected to have been impacted includes patient names, addresses, social security numbers, health information, medical records, bank records, financial account information, and drivers' license information.[23] This is precisely the type of data Netgain previously warned would be targeted by hackers and used to commit fraud. It is also the type of data Netgain warned its clients needed to be secured.

36. In January 2021, Netgain began notifying its clients of the Data Breach and that Sensitive Information may have been impacted.

37. For example, in a Notification Letter to Woodcreek Provider Services, LLC, Netgain reported "a security incident that involved unauthorized access to portions of the Netgain environment which Netgain had discovered in late November 2020 but may have occurred as early as September 2020." The cyber criminals launched a ransomware attack,

[22] Dissent, *Woodcreek Provider Notifies More than 210,000 Patients of Netgain Technology Ransomware Incident*, DataBreaches.net (Mar. 5, 2021), https://www.databreaches.net/woodcreek-provider-services-notifies-more-than-210000-patients-of-netgain-ransomware-incident/ /

[23] Lonut Llascu, *Netgain Ransomeware Incident Impacts Local Governments*, Bleeping Computer (Feb. 2, 2021), https://www.bleepingcomputer.com/news/security/netgain-ransomware-incident-impacts-local-governments/

encrypting the Sensitive Information of Netgain's clients and internal systems. In response, Netgain reported it took measures to contain the threat, including disabling external and internal network pathways and taking client services offline.[24]

38. On May 28, 2021, Caravus, an independent healthcare insurance broker in St. Louis, Missouri, issued a press release noting the "potential impact to some personal information as a result of a 2020 ransomware attack on a former vendor, Netgain Technology, LLC[.]"[25] Caravus's investigation revealed that, despite having previously ending its contract with Netgain, Netgain's servers still retained Caravus's data from in or before 2016. As one security blogger put it: "for more than 5 years, [Caravus's] data sat on an old server and Netgain never securely deleted it or encrypted it at rest[.]"[26] The attackers ultimately compromised that unsecured and unnecessarily stored data.

39. On August 24, 2021, LifeLong Medical Care, a health, dental, and social services provider in California's San Francisco Bay area, issued a press release noting "Netgain, a third-party vendor that provides services to certain healthcare providers, including LifeLong, discovered anomalous network activity."[27] LifeLong's investigation

[24] Ltr to Bob Ferguson, Office of the Attorney General of Washington State, from Barbara Nault, Studebaker Nault, PLLC (Feb. 17, 2021), https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/WoodcreekProviderServicesLLC.2021-02-17.pdf

[25] Dissent, *Caravus Impacted by Netgain Technology Breach*, DataBreaches.Net (May 28, 2021), https://www.databreaches.net/caravus-impacted-by-netgain-technology-breach-because-vendor-failure-to-destroy-legacy-data/

[26] *Id*.

[27] Press Release: LifeLong Medical Care Provides Notice of Netgain Data Security Incident (Aug. 24, 2021), https://lifelongmedical.org/wp-content/uploads/2021/08/LifeLong-Medical-Care-Notice-of-Data-Security-Incident.pdf

revealed "that certain identifiable personal and protected health information was accessed and/or acquired from Netgain's network in connection with this incident, including full names and one or more of the following: Social Security numbers, dates of birth, patient cardholder numbers, and/or treatment/diagnosis information."[28]

40. More than a year after the Data Breach, Netgain has continued to notify its clients of individuals whose Sensitive Information was compromised in the Data Breach. For example, on January 13, 2022, Entira, a Minnesota-based family medicine practice, issued notice to nearly 200,000 people informing them that Netgain's Data Breach may have compromised their Sensitive Information.[29] Additionally, on May 27, 2022, Perkins & Co. notified 354,647 that their information was impacted by Netgain's Data Breach.[30]

41. In all, at this time, the known Netgain customers impacted by the Data Breach include: (1) Ramsey County, Minnesota, (2) Woodcreek Provider Services and MultiCare Health System, (3) Sandhill Medical Foundation, (4) Apply Valley Clinic/ Alina Health, (5) Neighborhood Healthcare, (6) San Diego Family Care, and its associate, Health Center Partners of Southern California, (7) Jackson Thornton, (8) SouthCare Carolina, (9) Crystal Practice Management, (10) SAC Health Systems, (11) LifeLong Medical Care, (12) Perkins & Co; (13) Barrett Business Services; (14) Nevada Orthopedic & Spine Center; (15) Minnesota Community Care; and (16) Entira Family Clinics.

---

[28] *Id.*

[29] Jill, McKeon, *Family Medicine Practice Notifies Patients of Data Breach 1 Year Later*, Health IT Security (Jan. 18, 2022), https://healthitsecurity.com/news/family-medicine-practice-notifies-patients-of-data-breach-1-year-later

[30] *Perkins & Co. Announces Data Breach Related to Incident at Cloud-Hosting Company Netgain*, JDSupra.com (last visited, Jun. 16, 2022), https://www.jdsupra.com/legalnews/perkins-co-announces-data-breach-3372793/

42. Collectively, the impacted businesses have already reported hundreds of thousands of client and patient records impacted by the Data Breach. However, not all the impacted businesses have provided an indication of the number of records compromised, and it is likely other unknown or undisclosed entities were also affected.

43. What is clear, however, is that all the impacted companies provide healthcare or financial services, collect and maintain sensitive data, and trusted Netgain to do as it promised—to provide secure IT services that keep its data safe. Netgain failed to do so.

44. After the Data Breach, Netgain admitted its data security was deficient and caused the Data Breach to occur. For instance, Netgain acknowledged that it "identified additional opportunities to strengthen [its] security posture" and needed to "implement[] a number of . . . identified enhancements to [its] security posture . . . to progress a multi-pronged [security] approach[.]"[31] These measures purportedly included "deploy[ing] new tools, revised policies and enforcement procedures, and implement[ing] an advanced around-the-clock managed detection and response service for proactive threat monitoring."[32] Netgain also acknowledged a need to make "an ongoing commitment to ensure [data security] remains top-of-mind."[33]

45. Furthermore, while Netgain boasted of the "new tools" it implemented to increase its security posture, those tools were not new to the data security industry. Rather,

[31] *What We Learned as a Ransomware Victim – So You Don't Become One*, NetgainCloud.com (Mar. 24, 2021), https://netgaincloud.com/blog/what-we-learned-as-a-ransomware-victim-so-you-dont-become-one/
[32] *Id.*
[33] *Id.*

data security experts had been recommending those security measures be adopted for years leading up to the Data Breach.

46. For example, the "around the clock managed detection and response service" Netgain identified is part of the services provided by a Security Information and Event Monitoring System ("SIEM") designed to quickly identify indicators of an attack, issue warnings, and react to stop an intrusion early on. Data security experts have long recommended SIEM and other active monitoring systems in the healthcare industry to identify and respond to a data breach quickly and proactively.[34] Indeed, basic enterprise security monitoring, like Splunk, has been available since 2013.

47. Moreover, while Netgain now recognizes the need to make an "ongoing commitment" to data security and keep it "top-of-mind," security experts, including in the healthcare industry, have long warned companies that data security must be a top priority. The Department of Human Health and Services, in a series providing cybersecurity tips for those in the healthcare industry, wrote that:

> The tips in this document describe some ways to reduce the risk, decreasing the likelihood that patients' personal health information will be exposed to unauthorized disclosure, alteration, and destruction or denial of access. But none of these measures can be effective unless the health care practice is willing and able to implement them, to enforce policies that require these safeguards to be used, and to effectively and proactively train all users so that they are sensitized to the importance of information security. ***In short, each***

[34] Susan Biddle, Why SIEM Solutions Are Essential to Securing Healthcare Networks, Fortinet (Jun. 16, 2017), https://www.fortinet.com/blog/industry-trends/why-siem-solutions-are-essentialto-securing-healthcare-networks; Elizabeth O'Dowd, Healthcare SIEM Provides Security Through Even Data Monitoring, Hit Infrastructure (Dec. 31, 2017), https://hitinfrastructure.com/news/healthcare-siem-provides-security-through-event-datamonitoring.

> ***health care practice must instill and support a security-minded organizational culture.***[35](emphasis added).

48. Various notices have indicated the stolen Sensitive Information of Plaintiff and the Class included full names, dates of birth, bank account and routing numbers, Social Security numbers, driver's license numbers, medical records, health insurance policy numbers, and employee health information. For example, one version of the notice indicated the "information involved may have included some of the following: your name, date of birth, address, and information about the care you received from Neighborhood Healthcare such as insurance coverage information, physician you saw and treatment codes." Another stated that the "information involved…may include the following: name, date of birth, Social Security number, diagnosis/treatment information, provider name, medical record number, and treatment cost information." Similarly, a third notice indicated the data involved in the "cyberattack on Netgain's system included the following types of personal information: names, dates of birth, social security numbers, bank account and routing numbers, patient billing information and medical information, such as medical symptoms and diagnoses." Another stated that the data involved included:

> [F]ull or partial: first and last names, dates of birth, billing information, social security numbers, telephone numbers, mailing and billing addresses, email addresses, patient and record identifiers, information relating to [patient] treatment (including billing and diagnosis codes, and the dates and locations of [patient] treatment), information contained within [patient] state-issued photo identification (including biometric information such as [patient] height, weight, driver's license number, organ donor status, and appearance), and insurance cards containing [patient] name and/or beneficiary number.

---

[35] *Top 10 Tips for Cybersecurity in Healthcare*, Department of Health & Human Services (last visited Sept. 22, 2021), https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

49. However, the notice Netgain provided to some of its clients, including healthcare provider Health Center Partners of Southern California ("HCP"), was unreasonably delayed. Customers of this healthcare provider were not informed of the Data Breach until February 24, 2021, March 26, 2021, April 12, 2021, and May 7, 2021, although the breach "may have occurred as early as September 2020."[36] Hundreds of thousands of Class members were notified even later, including Plaintiff, who did not receive notice until well after the Data Breach. Plaintiff and some Class members did not know of the need to take action to secure their Sensitive Information and mitigate any associated risks or harm until more than a year after the breach occurred.

50. Similarly, Entira did not begin notifying victims of the Data Breach that their information had been compromised until January 2022, nearly one year after the breach occurred.[37]

Data Breaches Lead to Identity Theft and Cognizable Injuries.

51. The personal, health, and financial information of Plaintiff and the Class, is valuable and has been commoditized in recent years.

52. The ramifications of Defendant's failure to keep Plaintiff's and the Class's Sensitive Information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social

[36] Dissent, *Woodcreek Provider Notifies More than 210,000 Patients of Netgain Technology Ransomware Incident*, DataBreaches.net (Mar. 5, 2021), https://www.databreaches.net/woodcreek-provider-services-notifies-more-than-210000-patients-of-netgain-ransomware-incident/

[37] *See* https://ago.vermont.gov/wp-content/uploads/2022/04/2021-01-13-Entira-Family-Clinics-Family-Health-Services-MN-Data-Breach-Notice-to-Consumers.pdf.

Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

53. According to experts, one out of four data breach notification recipients becomes a victim of identity fraud.[38]

54. Stolen Sensitive Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

55. Moreover, according to Robert P. Chappell, Jr., a law enforcement professional, a minor's information can be stolen and used until the minor turns eighteen years old before the minor even realizes he or she has been victimized.[39]

56. The risk to minor Class members is substantial given their age and lack of established credit because their information can be used to create a "clean identity slate." It is not surprising, then, that one report found that children are 51% more likely be victims of identity theft than adults.[40] Cybercriminals on the dark web have been caught selling Social Security numbers of infants for $300 per number to be used on fraudulent tax returns.[41]

---

[38] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, ThreatPost.com (last visited, Feb. 21, 2013), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/

[39] Brett Singer, *What is Child Identify Theft?*, Parents, https://www.parents.com/kids/safety/tips/what-is-child-identity-theft/ (last visited July 28, 2021).

[40] Avery Wolfe, *How Data Breaches Affect Children*, Axion Cyber Sols. (Mar. 15, 2018), https://axiomcyber.com/data-breach/how-data-breaches-affect-children/.

[41] *Id.*

57. Once Sensitive Information is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional Sensitive Information being harvested from the victim, as well as Sensitive Information from family, friends, and colleagues of the original victim.

58. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

59. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiff and the Class that their Sensitive Information had been stolen.

60. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

61. Data breaches facilitate identity theft as hackers obtain consumers' Sensitive Information and use it to siphon money from existing accounts, open new accounts in the names of their victims, or sell consumers' Sensitive Information to others who do the same.

62. Victims of identity theft often suffer indirect financial costs as well, including the costs incurred due to litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit.

63. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their Sensitive Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

64. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Sensitive Information. To protect themselves, Plaintiff and the Class (and the business entities whose information was breached) will need to be remain vigilant against unauthorized data use for years or even decades to come.

65. After the Data Breach, Netgain attempted to downplay its role in causing the breach. Netgain began a series of blog posts billed as an effort to describe "what [Netgain] learned as a ransomware victim."[42] But the blogposts read as an effort to divert blame.

66. In one post, Netgain claimed that "[n]o company or government agency is immune to cyberattacks" and noted other, apparently larger organizations, were also breached.[43] It also put the blame, in part, on the very clients' whose data Netgain exposed. Netgain wrote that:

---

[42] *What We Learned as a Ransomware Victim – So You Don't Become One*, NetgainCloud.com (Mar. 24, 2021), https://netgaincloud.com/blog/what-we-learned-as-a-ransomware-victim-so-you-dont-become-one.

[43] *Id.*

> For too long, managed service providers and technology partners (including us) have taken the stance of shielding our clients from the headaches, intricacies, and complications that a strong security stance involves. While it's true that we can significantly reduce the burden of security on our clients and their teams, the responsibility is still shared. We owe it to our clients to ensure that they not only understand the steps we're taking as their IT partner, but also the measures that require their active participation and consent.[44]

67. In other words, despite Netgain's promise that it could and would protect its clients' highly sensitive data for them ("Hackers Don't Sleep. But you can."), after getting breached it claimed that *its clients* (who were not breached and who were not purportedly data security specialists) had a shared responsibility for the breach.

68. Thus, despite the fact Netgain, not its customers, is in complete control of its own systems and data security, it still has attempted to put the onus of data security onto its clients. This despite Netgain's supposed expertise in the matter and its representations that it would handle cybersecurity on their behalf.

69. Perhaps the most salient advice Netgain provided was in its third blog post, where it directed clients to "[a]ddress security requirements with third parties, particularly if the organization outsourced the management and control of some of its information systems, networks and/or desktop environment." Netgain—being the very type of third party that controls its clients' IT systems—deserves to be scrutinized and heavily monitored by its clients because, as evidenced by the Data Breach, it cannot be trusted to protect highly sensitive data.

70. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new (and valuable) form of currency. In a FTC roundtable presentation, former

[44] *Id.*

Commissioner, Pamela Jones Harbour, underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[45]

71. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[46] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry unapproved activity; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[47]

72. According to the FTC, unauthorized Sensitive Information disclosures wreak havoc on consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[48] The FTC, as such, treats the failure to employ reasonable

[45] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited September 22, 2021).

[46] *Start With Security, A Guide for Business*, FTC (last visited Sept. 22, 2021), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[47] *Id.*

[48] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012),://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited April 28, 2021).

and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

73. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded Netgain's Data Breach, further clarify the measures businesses must take to meet their data security obligations.

74. Consumers place a high value on their PII and a greater value on their PHI, in addition to the privacy of their Sensitive Information. Research shows how much

consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US $30.49–44.62."[49]

75. By virtue of the Data Breach here and unauthorized release and disclosure of the Sensitive Information of Plaintiff and the Class, Netgain deprived Plaintiff and the Class of the substantial value of their Sensitive Information, to which they are entitled. As previously alleged, Netgain failed to provide reasonable and adequate data security, pursuant to and in compliance with industry standards and applicable law.

76. As a cybersecurity expert, Netgain was aware of the potential harm caused by a data breach, and even offered cyber security best practices tips.[50] In fact, in its March 24, 2021 blog titled "What we learned as a ransomware victim – so you don't become one," Netgain writer Patrick Williamson admitted Netgain identified "additional opportunities to strengthen our security posture in a continuous journey with an ongoing commitment to ensure this remains top-of-mind."[51] Netgain, as a company profiting from its cybersecurity services, understood better than most how important data security is and the ongoing nature of maintaining the latest technology and protocols for cyber security.

---

[49] *See* Il-Horn Hann et al., *The Value of Online Information Privacy* (Oct. 2002) available at http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited September 22, 2021); *see also* Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22 (2) Information Systems Research 254, 254 (June 2011).

[50] *See* Kris Tufto, How Costly is a Data Breach (Mar. 3, 2020), https://netgaincloud.com/blog/how-costly-is-a-data-breach/

[51] *What We Learned as a Ransomware Victim – So You Don't Become One*, NetgainCloud.com (Mar. 24, 2021), https://netgaincloud.com/blog/what-we-learned-as-a-ransomware-victim-so-you-dont-become-one

77. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen.

78. As a result, victims suffer immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

79. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When Sensitive Information is stolen, accounts become less secure, and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

80. As a direct and proximate result of Netgain's wrongful actions and omissions here, Plaintiff and the Class have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*: (i) from the untimely and inadequate notification of the Data Breach, (ii) the resulting immediate and continuing risk of future ascertainable losses, economic damages and other actual injury and harm, (iii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; and (iv) out-of-pocket expenses for securing identity theft protection and other similar necessary services.

Defendant Failed to Adhere to HIPAA

81. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[52]

82. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI is properly maintained.[53]

83. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

[52] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[53] *See* 45 C.F.R. § 164.306 (Security standards and General rules); 45 C.F.R. § 164.308 (Administrative safeguards); 45 C.F.R. § 164.310 (Physical safeguards); 45 C.F.R. § 164.312 (Technical safeguards).

d. Failing to ensure compliance with HIPAA security standards by Defendant workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

Plaintiff's Experience

84. Plaintiff Yolanda Xiong. As a direct and proximate result of Netgain's wrongful actions and omissions, Plaintiff Xiong received a Notice that Plaintiff Xiong's Sensitive Information—stored on Netgain's systems—was stolen in the Data Breach. Netgain was storing Plaintiff Xiong's Sensitive Information on behalf of Entira, a family clinic system operating in Minnesota. Entira began notifying Plaintiff Xiong and other Data Breach victims in January 2022, more than a year after the Data Breach.

85. Entira's Notice disclosed that the information lost in the Netgain Data Breach included names, addresses, social security numbers and medical histories.

86. After receiving Notice, Plaintiff Xiong contacted Entira to request information on the Data Breach. During that call, an Entira representative told her everything was "okay," indicating Plaintiff Xiong need not worry about the Data Breach. But soon after her call with Entira, Plaintiff Xiong suffered identity theft.

87. In early 2022, Plaintiff Xiong received a letter from a credit bureau explaining that attempts were made to open credit card accounts in her name.

88. Given the exposure and theft of her data, Plaintiff Xiong remains at heightened risk for further harm.

CLASS DEFINITION AND ALLEGATIONS

89. Plaintiff brings this class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following classes:

The Nationwide Class:

> All natural persons residing in the United States whose data was exposed as a result of the Data Breach.

The Minnesota Subclass:

> All natural persons residing in the State of Minnesota whose data was exposed as a result of the Data Breach.

The Nationwide Class and Minnesota Subclass are referred to as "the Class," unless there is need to differentiate them. Excluded from the Class are: (i) Defendant and its officers, directors, affiliates, parents, and subsidiaries (ii) the Judge presiding over this action, and (iii) any other person or entity found by a court of competent jurisdiction to be guilty of initiating, causing, aiding or abetting the criminal activity occurrence of the Data Breaches or who pleads nolo contendere to any such charge.

90. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

91. **Numerosity**. The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiff is informed and believes that the proposed Class includes hundreds of thousands of Defendant's clients' customers and patients who have been damaged by Defendant's conduct as alleged herein. The precise number of Class members is unknown to Plaintiff but may be ascertained from Defendant's records.

92. **Commonality and Predominance**. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members. These common legal and factual questions include, but are not limited to, the following:

a. whether Defendant engaged in the wrongful conduct alleged herein;

b. whether the alleged conduct constitutes violations of the laws asserted;

c. whether Defendant owed Plaintiff and the other Class members a duty to adequately protect their Sensitive Information;

d. whether Defendant breached its duty to protect the personal and financial data of Plaintiff and the other Class members;

e. whether Defendant knew or should have known about the inadequacies of its data protection, storage, and security;

f. whether Defendant failed to use reasonable care and commercially

reasonable methods to safeguard and protect Plaintiff's and the Class's Sensitive Information from unauthorized theft, release, or disclosure;

g. whether the proper data security measures, policies, procedures and protocols were in place and operational within Defendant's offices and computer systems to safeguard and protect Plaintiff's and the Class's Sensitive Information from unauthorized theft, release or disclosure;

h. whether Defendant breached its promise to keep Plaintiff's and the Class's Sensitive Information safe and to follow federal data security protocols;

i. whether Defendant's conduct was the proximate cause of Plaintiff's and the other Class's injuries;

j. whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

k. whether Plaintiff and the Class suffered ascertainable and cognizable injuries as a result of Defendant's misconduct;

l. whether Plaintiff and the Class are entitled to recover actual damages and/or statutory damages; and

m. whether Plaintiff and the Class are entitled to other appropriate remedies, including injunctive relief.

93. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiff on behalf of herself and the Class. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

94. **Typicality**. Plaintiff's claims are typical of the claims of the members of the Class. All Class members were subject to the Data Breach and had their Sensitive Information accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class members in a similar manner.

95. **Adequacy**. Plaintiff will fairly and adequately protect the interests of the members of the Class, has retained counsel experienced in complex consumer class action litigation, and intends to prosecute this action vigorously. Plaintiff has no adverse or antagonistic interests to those of the Class.

96. **Superiority**. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for the Class members, on an individual basis, to obtain effective redress for the wrongs done to them. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts and would also increase the delay and expense to all parties and the courts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff, the Nationwide Class, and the Minnesota Subclass)

97. Plaintiff incorporates by reference all previous allegations as though fully set

forth herein.

98. Netgain owed to Plaintiff and the Class a duty of reasonable care to protect Plaintiff's and the Class's data from the foreseeable threat of theft during a Data Breach. This duty arose from several sources.

99. Netgain owed this duty to Plaintiff and the Class because Plaintiff and the Class are a well-defined, foreseeable, and probable group of individuals whom Netgain should have been aware could be injured by Defendant's inadequate security protocols. Netgain actively solicited clients who retained managed Sensitive Information and, as part of its services, Netgain took control and managed that Sensitive Information on behalf of its clients. Thus, for Netgain to provide its services, it was required to use, handle, gather, and store the Sensitive Information of Plaintiff and the Class. A repository of highly Sensitive Information was, as Netgain counseled its clients, a significant target for hackers. Netgain, thus, knew and understood long before the Data Breach that, as the keeper of Sensitive Information, it would need to implement adequate data security measures to protect against a Data Breach. The foreseeable harm to Plaintiff and the Class of Netgain's inadequate data security measures created a duty to act reasonably in security Sensitive Information.

100. Additionally, Netgain assumed a duty to Plaintiff and the Class to protect their sensitive data. Netgain represented to its clients—healthcare and financial service companies—that it could collect, manage, store, and secure their customers' data, including representing that it used "DoD-grade" and "ultra-secure" technologies to protect sensitive data. As such, when those healthcare and financial services companies provided Netgain

with Plaintiff's and the Class's Sensitive Information, it had a duty to protect that Sensitive Information based on its representations that it could and would do so and on its knowledge that a repository of sensitive data would be targeted by hackers.

101. Netgain also owed a duty to timely and accurately disclose the scope, nature, and occurrence of the Data Breach. This disclosure is necessary so Plaintiff and the Class can take appropriate measures to avoid unauthorized use of their Sensitive Information, accounts, cancel and/or change usernames and passwords on compromised accounts, monitor their accounts to prevent fraudulent activity, contact their financial institutions about compromise or possible compromise, obtain credit monitoring services, and/or take other steps in an effort to mitigate the harm caused by the Data Breach and Netgain's unreasonable misconduct.

102. Netgain breached its duty to Plaintiff and the Class by failing to implement and maintain reasonable security controls that were capable of adequately protecting the Sensitive Information of Plaintiff and the Class.

103. Netgain also breached its duty to timely and accurately disclose to the clients, Plaintiff and the Class that their Sensitive Information had been or was reasonably believed to have been improperly accessed or stolen.

104. Netgain's negligence in failing to maintain reasonable data security is further evinced by its failure to comply with legal obligations and industry standards, and the delay between the date of the Data Breach and the time when Netgain disclosed it.

105. The injuries to Plaintiff and the Class were reasonably foreseeable to Netgain because laws and statutes, and industry standards require it to safeguard and protect its

computer systems and employ procedures and controls to ensure that unauthorized third parties did not gain access to Plaintiff's and the Class's Sensitive Information.

106. The injuries to Plaintiff and the Class were reasonably foreseeable because Netgain knew or should have known that systems used for safeguarding Sensitive Information were inadequately secured and exposed consumer Sensitive Information to being breached, accessed, and stolen by hackers and unauthorized third parties. As such, Netgain's own misconduct created a foreseeable risk of harm to Plaintiff and the Class.

107. Netgain's implemented knowingly deficient data security measures and failed to adopt reasonable measure that could protect the Sensitive Information of Plaintiff and the Class, and those deficient security measures proximately caused Plaintiff's and the Class's injuries because they directly allowed hackers to easily access Plaintiff's and the Class's Sensitive Information. This ease of access allowed the hackers to steal Sensitive Information of Plaintiff and the Class, which could lead to dissemination in black markets.

108. As a direct proximate result of Netgain's conduct, Plaintiff and the Class have suffered theft of their Sensitive Information. Netgain allowed thieves access to Class's Sensitive Information, thereby decreasing the security of the Class's financial and health accounts, making Class's identities less secure and reliable, and subjecting the Class to the imminent threat of identity theft. Not only will Plaintiff and the Class have to incur time and money to re-secure their bank accounts and identities, but they will also have to protect against identity theft for years to come.

109. Netgain's conduct warrants moral blame because it actively solicited its services to its clients, wherein it used, handled and stored the Sensitive Information of

Plaintiff and the Class without disclosing that its security was inadequate. Holding Netgain accountable for its negligence will further the policies embodied in the law by incentivizing IT service providers to properly secure sensitive consumer information and protect the consumers who rely on these companies every day.

SECOND CAUSE OF ACTION
Declaratory Judgment
(On Behalf of the Plaintiff and all Classes)

110. Plaintiff incorporates by reference all previous allegations as though fully set forth herein.

111. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious and which violate the terms of the federal and state statutes described above.

112. An actual controversy has arisen in the wake of the Data Breach at issue regarding Netgain's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiff alleges Netgain's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

113. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Netgain owed, and continues to owe, a legal duty to employ reasonable data security to secure the Sensitive Information with which it is entrusted, specifically including information pertaining to healthcare and financial records it obtains from its clients, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Netgain breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Netgain's breach of its legal duty continues to cause harm to Plaintiff and the Class.

114. The Court should also issue corresponding injunctive relief requiring Netgain to employ adequate security protocols consistent with industry standards to protect its clients' (i.e. Plaintiff's and the Class's) data.

115. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Netgain's data systems. If another breach of Netgain's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

116. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Netgain if an injunction is issued.

117. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all others similarly situated, respectfully requests that the Court enter an order:

a. Certifying the Class and Subclasses as requested herein;

b. Appointing Plaintiff as Class Representative and undersigned counsel as Class Counsel;

c. Finding that Defendant engaged in the unlawful conduct as alleged herein;

d. Enjoining Defendant's conduct and requiring Defendant to implement proper data security practices, specifically:

   i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

   ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

   iii. requiring Defendant to delete, destroy, and purge the Sensitive Information of Plaintiff and the Class unless Defendant can provide

to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and the Class's Sensitive Information;

v. prohibiting Defendant from maintaining Plaintiff's and the Class's Sensitive Information on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's

network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Sensitive Information, as well as protecting the Sensitive Information of Plaintiff and the Class;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting Sensitive Information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats,

both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential Sensitive Information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers;

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class and Subclasses, and to report any deficiencies with compliance of the Court's final judgment;

xviii. requiring Defendant to design, maintain, and test its computer systems to ensure that Sensitive Information in its possession is adequately secured and protected;

xix. requiring Defendant to disclose any future data breaches in a timely and accurate manner;

xx. requiring Defendant to implement multi-factor authentication requirements;

xxi. requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; and

xxii. requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class members.

e. Awarding Plaintiff and Class damages;

f. Awarding Plaintiff and Class pre-judgment and post-judgment interest on all amounts awarded;

g. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiff, on behalf of herself and the Class, demands a trial by jury on all issues so triable.

Dated: July 20, 2022

Respectfully submitted,

By: */s/ Raina C. Borrelli*

Raina C. Borrelli
Samuel J. Strauss
Brittany Resch
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
raina@turkestrauss.com
sam@turkestrauss.com
brittanyr@turkestrauss.com